In the Claims:

Please amend the Claims as follows and without prejudice. This listing of Claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims

1. (CURRENTLY AMENDED) A method ~~for selecting at least one encryption key used~~ to encrypt a data message having ~~at least one~~ a plurality of message data ~~block~~ blocks prior to transmitting said ~~encrypted~~ message data blocks over a network, said method comprising ~~the steps of~~:

[[a.]] extracting a data value from [[a]] one of said message data ~~block~~ blocks;

[[b.]] selecting an encryption key from among a plurality of encryption [[key]] keys dependently upon said extracted data value; and,

[[c.]] encrypting a subsequent one of said message data ~~block~~ blocks using said selected encryption key. ~~; and~~

~~d. transmitting said encrypted data block over said network~~

2. (CURRENTLY AMENDED) The method as recited in claim 1, wherein ~~steps a-d~~ said extracting, selecting and encrypting are iteratively repeated for each of said message data ~~block~~ blocks.

3. (CURRENTLY AMENDED) The method as recited in claim 1, further comprising ~~the steps of~~ :

[[a.]] receiving said encrypted message data ~~blocks~~ block;

[[b.]] decrypting said received message data block using [[an]] a key based on a prior data block;

[[c.]] extracting a data value from [[a]] said decrypted message data block; and

[[d.]] selecting an encryption key from among a plurality of retained encryption keys dependently upon said extracted value for said decrypted message data block.

4. (CURRENTLY AMENDED) The method as recited in claim 1, wherein said extracted [[a]] data value is determined using a known number of bits.

5. (CURRENTLY AMENDED) The method as recited in claim 4, wherein said known number of bits are distributed among at least one byte of said one of said message data ~~block~~ blocks.

6. (CURRENTLY AMENDED) The method as recited in claim 4, wherein said known number of bits are located in a first byte of ~~each of said message blocks~~ said one of said message data blocks.

7. (CURRENTLY AMENDED) The method as recited in claim 4, wherein said known number of bits are located in a last byte of ~~each of said message blocks~~ said one of said message data blocks.

8. (CURRENTLY AMENDED) The method as recited in claim [[1]] 3, wherein said received message data block corresponds to at least one unencrypted message data block.

9. (CURRENTLY AMENDED) The method as recited in claim [[1]] 3, wherein said received message data block corresponds to a synchronizing indicator.

10. (CURRENTLY AMENDED) The method as recited in claim 1, wherein said step of extracting further comprises limiting said extracted data value to a known range.

11. (CURRENTLY AMENDED) The method as recited in claim 10, wherein said known range is determined using modulo-arithmetic.

12. (CURRENTLY AMENDED) The method as recited in claim 10, wherein said known range is ~~substantially comparable to~~ associated with a number of said stored encryption keys.

13. (CURRENTLY AMENDED) A system for selecting at least one encryption key used to encrypt a data message having ~~at least one~~ a plurality of message data ~~block~~ blocks prior to transmitting said ~~encrypted~~ message data blocks over a network, said system comprising:

a communication apparatus operative to:

extract a data value from [[each]] one of said ~~at least one~~ message data blocks;

select an encryption key from among a plurality of encryption [[key]] keys stored in a memory dependently upon said extracted data value; and, encrypt at least [[one]] a subsequent one of said message data ~~block~~ blocks using said selected encryption key.~~; and~~

~~transmit said encrypted message data block over said network.~~

14. (CURRENTLY AMENDED) The system as recited in claim 13, further comprising:

a second communication apparatus operative to:

receive said ~~at least one transmitted~~ encrypted message data block;

extract a data value from ~~each of said~~ a previously ~~transmitted~~ received message data ~~blocks~~ block;

select [an] a decryption key from among a plurality of decryption keys stored said memory based on said extracted data value from said previously received message data block; and

decrypt said ~~at least one~~ received encrypted message data block using said selected key.

15. (CURRENTLY AMENDED) The system as recited in claim 13, wherein said extracted [[a]] data value is determined using a known number of bits.

16. (CURRENTLY AMENDED) The system as recited in claim 15, wherein said known number of bits are distributed among at least one byte of said previously received message data block.

17. (CURRENTLY AMENDED) The system as recited in claim 15, wherein said known number of bits are located in a first byte of ~~each of~~ said previously received message ~~blocks~~ data block.

18. (CURRENTLY AMENDED) The system as recited in claim 15, wherein said known number of bits are located in a last byte of ~~each of said message blocks~~ said previously received message data block.

19. (CURRENTLY AMENDED) The system as recited in claim [[13]] 14, wherein said received message data block corresponds to at least one unencrypted message data block.

20. (CURRENTLY AMENDED) The system as recited in claim [[13]] 14, wherein said received message data block corresponds to a synchronization indicator.

21. (CANCELLED)

22. (CURRENTLY AMENDED) The system as recited in claim [[21]] 13, wherein said apparatus is further operative to limit said extracted data value to a known range.

23. (CURRENTLY AMENDED) The system as recited in claim 22, wherein said known range is ~~substantially comparable to~~ associated with a number of said plurality of encryption keys.

24. (CURRENTLY AMENDED) A device for use with ~~to determine at least one encryption key from~~ a plurality of encryption keys [[,]] stored in a memory, ~~said encryption key~~ and useful for [[used to encrypt]] encrypting a message composed of data message blocks, said device ~~comprised of~~ comprising:

a processor, in communication with said memory, operative to:

extract a known number of data bits from [[a]] one of said data message ~~block~~ blocks;

select an encryption key from said stored encryption keys based on the content of said ~~known number of~~ extracted data bits; and

encrypt a subsequent one of said data message ~~data block~~ blocks using said selected encryption key; and

a transmitting device, in communication with said processor, to transmit said encrypted data message block.

25. (CURRENTLY AMENDED) The device as recited in claim 24, further comprising:

a receiving device to receive [[a]] said transmitted data message block;

a processor, in communication with said receiving device, operative to:

extract said known number of data bits from a previously received one of said data message ~~data block~~ blocks;

select a decryption key from a plurality of decryption keys stored in said memory based on ~~content of a known data item~~ said extracted data bits from said received on of said data message blocks; and

decrypt said received data message block using said selected decryption key.

26. (CURRENTLY AMENDED) The device as recited in claim 24, wherein said ~~known number of~~ extracted data bits are distributed among at least one byte of said one of said data ~~block~~ message blocks.

27. (CURRENTLY AMENDED) The device as recited in claim 24, wherein said ~~known number of~~ extracted data bits are located in a first byte of ~~each of~~ said one of said ~~message~~ data message blocks.

28. (CURRENTLY AMENDED) The device as recited in claim 24, wherein said ~~known number of~~ extracted data bits are located in a last byte of ~~each of~~ said one of said ~~message~~ data message blocks.

29. (CURRENTLY AMENDED) The device as recited in claim 24, wherein said encrypted data message block corresponds to at least one unencrypted data message block.

30. (CURRENTLY AMENDED) The device as recited in claim 29, wherein said encrypted data message block further corresponds to a synchronization indicator.

31. (CURRENTLY AMENDED) The device as recited in claim 24, wherein said processor is further operative to limit said extracted data value to a known range.

32. (CURRENTLY AMENDED) The device as recited in claim 31, wherein said known range is ~~substantially comparable to~~ associated with a number of said plurality of encryption keys.